Contactless transmission of intellectual property data to protect FPGA designs

L Bossuet, V Fischer, P Bayon

Contactless Transmission of Intellectual Property Data to Protect FPGA Designs

L. Bossuet, V. Fischer
Laboratoire Hubert Curien, CNRS UMR 5516
Université Jean Monnet
42000 Saint-Etienne, France
Lilian.bossuet@univ-st-etienne.fr

P. Bayon
Brightsight
Delft, 2628, The Netherlands
bayon@brightsight.com

Abstract— **Over the past 10 years, the designers of intellectual properties (IP) have faced increasing threats including illegal copy or cloning, counterfeiting, reverse-engineering. This is now a critical issue for the microelectronics industry, mainly for fabless designers and FPGA designers. The design of a secure, efficient, lightweight protection scheme for design data is a serious challenge for the hardware security community. In this context, this paper presents the first ultra-lightweight transmitter using side channel leakage based on electromagnetic emanation to send embedded IP identity discreetly and quickly. In addition, we present our electromagnetic test bench and a coherent demodulation method using slippery window spectral analysis to recover data outside the device. The hardware resources occupied by the transmitter represent less than 0.022% of a 130 nm Microsemi Fusion FPGA. Experimental results show that the demodulation method success to provide IP data with a bit rate equal to 500 Kbps.**

Keywords—IP protection; side channel; electromagnetic emanation analysis;

I. INTRODUCTION

For digital circuit design the re-use of embedded intellectual properties (IP) is more and more important due to prohibitive cost of ASIC design. Nevertheless the IP business suffers from a lack a security due to the intrinsic form of IPs sales and exchanges. Many dedicated threats target the IP life cycle and result to revenues losses for the IP designers [1]. The IP threat model includes illegal re-use, illegal sales, cloning (illegal copy) of the IP. The extent of threats targeting IPs is linked to the type of IP: software IPs (typically hardware description language files), firmware IPs (*synthesized* netlist), and hardware IPs (FPGA bitstream or physical layout).

One of the solutions for the IP designers to protect their intellectual property is to be able to detect the presence of a copy of an IP embedded in a digital device by using IP identification. Works on IP watermarking and IP fingerprinting try to provide the IP identification service. But, most of the time the published solutions are not practical mainly because of the complexity of the watermarking/fingerprinting verification scheme [2]. Efficient IP identification scheme needs to be contactless, rapid and ultra-lightweight. Up to now, these three characteristics are not available in the state-of-the-art. To meet these requirements, in this paper we propose an ultra-lightweight binary frequency shift keying (BFSK) transmitter to forward IP identity (that could generated for example by a feedback shift-register or a physical unclonable function [1]) discreetly using an electromagnetic channel. Such circuit is usually called “spy circuitry”. Using the electromagnetic channel, it is possible to contactless check the presence of an IP inside a digital device.

The rest of this paper is organized as follows. In Section 2, we present related works. In Section 3, we detail the proposed electromagnetic communication of data (i.e. IC/IP information). In Section 4, we present a method to analyze the electromagnetic spectrum to BFSK signal demodulation. In Section 5, we compare published spy circuitries that use a side-channel for IP protection and hardware Trojans. In Section 6, we present two industrial scenarios for the use of the proposed IP protection scheme and in Section 7 we present our conclusions.

II. RELATED WORK

Well-known threat in cryptographic engineering is side channel attacks [3], [4]. Most of the dynamic characteristics of both hardware and software implementations of cryptographic primitives can be used for side channel analysis: computation time, power consumption, electromagnetic radiation, optical radiation, even the sound produced during computation. These side channels can be used as transmission channels to send intellectual property data from a device or an embedded IP. For example in [5], the thermal channel representing a contactless communication was used to transfer information from an embedded tag to a remote receiver. However the embedded thermal tag used in this commercial solution requires a relatively large area (255 Spartan-3 slices). In [6], the authors propose using two shift registers to generate a recognizable signature-dependent power consumption pattern to reveal the IP signature. Power consumption was also used in [7] to communicate the IP identity. To reinforce such work, the authors of [8] propose using the power supply signal of an IP as a physical hash function for fingerprinting.

Related works can be found also in the malicious hardware design such as hardware Trojans. Such systems use side channels to forward secret information such as a symmetric cipher key from cryptographic hardware implementation [9],

[10], but also to cause or amplify side-channel leakage of cryptographic hardware [11].

Expect [5], all the related works use power consumption as a communication channel which is not contactless. Unlike the proposed solution, all the related works are not lightweight and rapid as the section 5 of this paper will show.

III. PROPOSED EM COMMUNICATION OF IP DATA

Electromagnetic radiation is an efficient side channel since, unlike measurement of power consumption, electromagnetic radiation can be measured locally. One of the main advantages of this side channel is that it is impossible to hide the leak concerning electromagnetic radiation by using a global countermeasure. Moreover the electromagnetic test bench is not expensive (less than US$ 10K without an oscilloscope, which is the most expensive component). Last but not least, a spectral analysis of the electromagnetic radiation provides information on the oscillating structure such as a ring-oscillator [12]. For all these reasons, we use the electromagnetic channel for our IP identification scheme. To this end, we designed an ultra-lightweight BFSK transmitter which could be activated outside the device by an ID checker or internally by a specific event (e.g. specific input sequence, internal data value, system state). Note that an enable signal is required to reduce the power consumed by the ring oscillator. Moreover, a permanently activated transmitter could be detected more easily by a spectral analysis of electromagnetic emanations of the device and could also cause local heating and premature aging of the chip.

BFSK is one of the common modulation schemes used in digital communication. The binary data are sent using a sinusoidal carrier at two frequency tones f_0 and f_1, representing high ('1') and low ('0') logic levels. The binary data arriving at the transmitter input at certain bitrates determine the commutation of the tones at the transmitter output. The proposed BFSK transmitter uses a dedicated configurable ring-oscillator, as shown in Fig. 1. The configurable ring-oscillator is designed using one multiplexor, $N+K$ delay elements, and a feedback chain controlled by a NAND gate for activation of transmission to reduce power consumption. Actually, the transmitter is used only during a short time when the enable signal is high, and it consumes power only during this small piece of time. The power consumption of this transmitter is thus completely negligible.

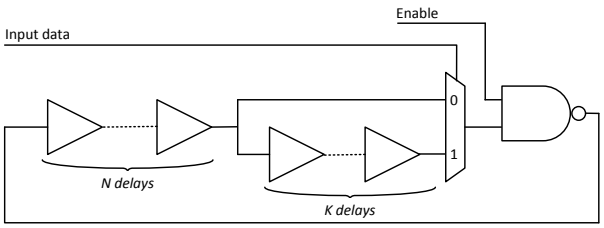

Fig. 1. Architecture of the ultra-lightweight digital BFSK transmitter based on a configurable ring oscillator.

Input data controls the multiplexor, as shown in Fig. 1. When input data is low, the ring oscillator uses N delays and its oscillation frequency is f_0. When input data is high, the ring oscillator uses $N+K$ delays and its oscillation frequency is f_1. Since the ring oscillator's oscillation frequency decreases with an increase in the number of delay elements, frequency f_0 is higher than frequency f_1. These two frequencies have to be selected according to the bandwidth of the electromagnetic analysis platform, which is used to acquire and measure the transmitted signal. The bandwidth of our test bench, which is described in Section 4, was limited to 100 MHz and 1 GHz by the low-noise amplifier.

The proposed BFSK transmitter was implemented in Microsemi FUSION flash based FPGA (130 nm CMOS technology) containing 600K logic gates (M7AFS600). The device contains 13 824 tiles, each tile can be used to implement one D-flip-flop or one configurable multiplexor-based logic block implementing any 3-input logic function.

The configurable number of delays in the ring oscillator of the proposed BFSK transmitter makes it possible to select precisely the two frequencies f_0 and f_1 using parameters N and K. Table I lists the ring oscillator frequencies and the number of Fusion tiles used by the BFSK transmitter for five values of N and K, with N ranging from 0 to 4, and K ranging from 1 to 5. According to Table I, f_0 can be chosen between 119 MHz ($N=4$) and 385 MHz ($N=0$) and f_1 can be chosen between 70 MHz ($N=4$, $K=5$) and 280 MHz ($N=0$, $K=1$). The exact value of f_0 depends on the number of delay elements, but also on the placement and routing of the transmitter. For the values N and K listed in Table I, the frequency variation was less than 1.7% (the maximum frequency deviation in Table I is 2 MHz when $N = 4$).

TABLE I. HARDWARE IMPLEMENTATION RESULTS OF THE BFSK TRANSMITTER

N	K	f_0 (MHz)	f_1 (MHz)	Fusion Tiles	LUT4	EG
0	1	385	280	3	2	4.67
	2	383	210	4	3	5.34
	3	384	151	5	4	6.01
	4	385	130	6	5	6.68
	5	381	111	7	6	7.35
1	1	272	189	4	3	5.34
	2	272	156	5	4	6.01
	3	270	120	6	5	6.68
	4	271	106	7	6	7.35
	5	269	93	8	7	8.02
2	1	168	144	5	4	6.01
	2	169	124	6	5	6.68
	3	169	100	7	6	7.35
	4	168	91	8	7	8.02
	5	168	79	9	8	8.69
3	1	146	128	6	5	6.68
	2	147	112	7	4	7.35
	3	146	92	8	5	8.02
	4	145	84	9	6	8.69
	5	144	74	10	7	9.36
4	1	123	110	7	6	7.35
	2	121	98	8	7	8.02
	3	122	83	9	8	8.69
	4	121	77	10	9	9.36
	5	119	70	11	10	10.03

The number of tiles used by the BFSK transmitter is very low, i.e. from 3 tiles (*N=0, K=1*) to 11 tiles (*N=4, K=5*). These values are equivalent to less than 0.022% and less than 0.080% of the total number of tiles included in the targeted 600K-gate FUSION FPGA, respectively. This very small number of tiles is very promising for good dissimulation of the BFSK transmitter inside the sea of gates/tiles. In order to estimate the number of resources needed for implementation with Xilinx SRAM FPGA or Altera SRAM FPGA, Table I gives the number of 4-input look-ups (LUT4) used by the BFSK transmitter with such FPGAs.

To evaluate the logical resources needed by the BFSK transmitter in ASIC implementations, the right hand column in Table I gives the number of equivalent gates (EG) in the transmitter. The gate count was estimated using the Virtual Silicon standard cell library based on the UMC L180 0.18 µm 1P6M Logic process (UMCL18G212T3 [13]). The delay gates are replaced by more efficient standard NOT gates. The gate count of a standard NOT gate is 0.67 EG, and that of the standard multiplexor, 2.33 EG. The standard NAND gate uses 1 EG. So the number of gates of the whole BFSK transmitter ranges from 4.67 EG (*N = 0, K = 1*) to 10.03 EG (*N = 4, K = 5*). Note that one flip-flop requires between 5.33 EG and 12.33 EG to store a single bit [13].

Such a transmitter is clearly ultra-lightweight in both FPGA and ASIC implementations. The small logical resources requirement of the proposed spy circuitry makes reverse engineering it harder, although not impossible [15]. Even with recent CMOS technologies, the attacker can reverse engineer ICs using a scanning electron microscope and an automatic tool for circuitry extraction [15], [16]. Nevertheless, the smaller the piece of hardware used for BFSK transmitter the harder it is to detect during reverse engineering. Detection of the transmitter using standard Trojan detection methods [17], [18] is not feasible because the transmitter does not change the data path of the circuit and because of the ultra-low signal-to-noise ratio on the electromagnetic channel, as shown in our experimental results below (Section 4).

IV. Experimental Results

The electromagnetic radiation of the device was evaluated using the near-field electromagnetic analysis test bench described in [12]. The border between the far field and the near field can be considered to be about 23 mm from the device, depending on the hardware concerned. The most important part of the test bench is the acquisition chain. It determines the signal to noise ratio and measurement precision.

The chain, as presented Fig. 2, is composed of:

- A Langer magnetic probe with a frequency range of from 30 MHz to 3 GHz and a spatial resolution of approximately 500 µm.
- A Miteq low-noise amplifier with a frequency range of from 100 MHz to 1 GHz.
- A LeCroy oscilloscope with a frequency range of up to 3.5 GHz and a sampling rate of up to 40 GS/s.

As presented in Fig. 2, the device to be tested (the board) is fixed to a XYZ table with repeatability of movement of 1 µm. The test bench, including the acquisition chain, XYZ table, FPGA configuration and power supply variations, is controlled by a computer.

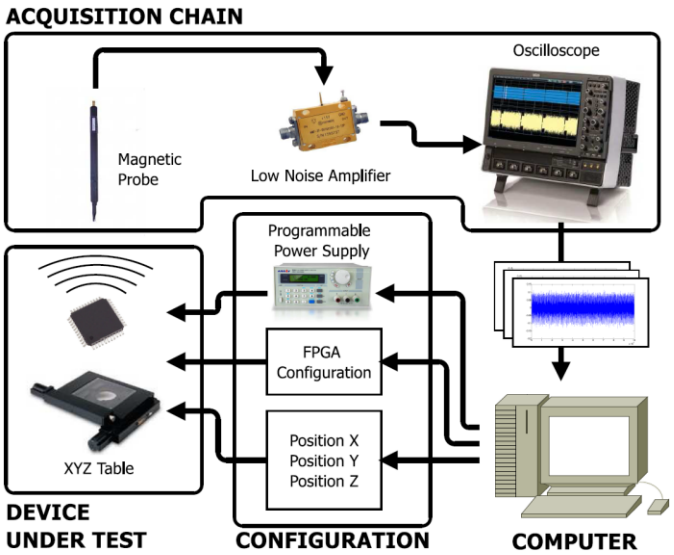

Fig. 2. Near-field Electromagnetic analysis test bench.

Electromagnetic analysis of IC is contactless, local, and can be spatial or/and temporal. This last point makes it possible to perform frequency analysis of the electromagnetic emanation. In the your bench the spectral range is limited to 100 MHz and 1 GHz. Standard devices aimed at direct BFSK demodulation cannot be used for these relatively high frequencies. Available integrated BFSK demodulators are limited to a few dozen megahertz. For this reason, we developed a dedicated BFSK demodulation scheme for our needs, in which a spectral analysis of the low noise amplifier output (a component of the test bench) is performed to measure the f_0 and f_1 spectral contribution. The transmitted high (low) level is detected when f_1 spectral contribution is higher (lower) than that of f_0.

Fig. 3 illustrates the spectral analysis of the BFSK transmitter's electromagnetic emission when *N = 1* and *K = 1*, which corresponds to a small transmitter with high frequencies in Table I. For the spectral analysis, a 16 384 points FFT was computed. Fig. 3 presents a zoom (X and Y axis) on the global spectrum of the local EM emanation of the circuit when the BFSK transmitter sends a '0' (*in blue*) and when the BFSK transmitter sends a '1' (in red). Notice also that we placed a small antenna in the close vicinity of the ring. The amplitude of the spectral rays at 180, 200, 220, 240, 260, 280 MHz are very high compared to the two spectral rays at 189.2 MHz and 272.2 MHz. However, we have cut the upper part of the spectrum in order to see the two interesting rays (at 189.2 MHz and 272.2 MHz). These frequencies correspond to the spectral contribution of the BFSK frequencies f_0 and f_1. Actually, according to Table I, for Microsemi FUSION FPGA, the frequency f_0 is around 272 MHz and f_1 is around 189 MHz. Slight variations in the frequency values (around the values presented in Table I) are due to environmental variations (mainly temperature). These variations are too small to

jeopardize the success of demodulation because the BFSK designer knows the chosen parameters *N* and *K* and targeted frequencies f_0 and f_1 for transmission of low and high levels.

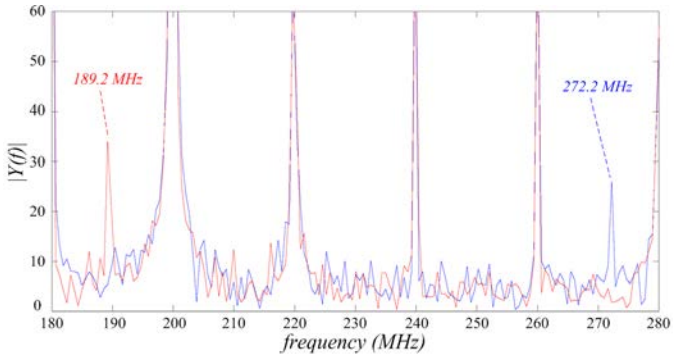

Fig. 3. Parts (zoom in x-axis and y-axis) of the electromagnetic emanation spectral analysis of the proposed BFSK transmitter when it sends a high level at f_1=189.2MHz (in red) and when it sends a low level at f_0=272.2 MHz (in blue).

Without knowledge of the BFSK parameters, the electromagnetic transmission cannot be easily detected because it cannot be distinguished from spectral noise. The signal-to-noise ratio of the BFSK transmission in Fig. 3 is -135 dB for a 1 GHz bandwidth. Such an ultra-low SNR represents efficient protection against unwanted BFSK transmitter detection via a side channel. However, knowing the *N* and *K* parameters, the BFSK designer can calibrate the demodulation (determine the two frequencies) by electromagnetic analysis of the ring oscillators based on the differential spectral analysis as described in [12].

The spectral contribution of the two BFSK frequencies during transmission (which is limited by the transmitter enable signal) at the low-noise amplifier output is measured to determine the transmitted bit sequence. In order to apply the demodulation technique described here, called coherent demodulation, theoretically the bitstream rate (bitrate) is limited to 0.5 times the frequency difference between f_0 and f_1. In the case shown in Fig. 3, theoretically the maximum bitrate is 41.5 Mbps (theoretically limited to 53 Mbps when $N = 0$ and $K = 1$). The coherent demodulation scheme cannot be used for higher bitrates, instead more sophisticated and more expensive demodulation techniques should be used. To reduce the size of the BFSK transmitter, a time-interleaving transmitter should be used to increase the bitrate. However, the high transmission rate is not so important, because data (e.g. IP identifier or stolen data) can be stored at a higher data rate before being transmitted at a slower rate. The small area and unobtrusiveness of the BSFK transmitter are much more important properties than transmission rate.

For the coherent demodulation of the electromagnetic radiation, we propose a slippery window spectral analysis. Indeed, overall spectral analysis masks the effects of the nonstationarity of the signal and therefore provides no information about its temporal evolution. Slippery window spectral analysis is a three-dimensional representation of the signal: amplitude, frequency, and time. It requires two quantities *Fw*, the width of the FFT window frame and the difference $\Delta\tau$ between two frames. For our experiment, we chose *Fw* equal to 16 384 points (2^{14}-point FFT) and $\Delta\tau$ equal to 100 points. For each frame, the FFT provides the software demodulator with the amplitude of signals f_0 and f_1 which enables the demodulator to distinguish between a transmitted '1' or '0'.

To illustrate data transmission from the circuit via the EM channel, we used a shift register that stored the following 16-bit sequence: "1011110111011100". The clock frequency of the shift register is 500 kHz. When the enable signal of the transmitter is given, the sequence is sent cyclically to the BFSK transmitter, which transmits it via the electromagnetic channel. Fig. 4 gives the result of the coherent demodulation obtained at a 500 Kbps bit rate, which served as a proof of concept.

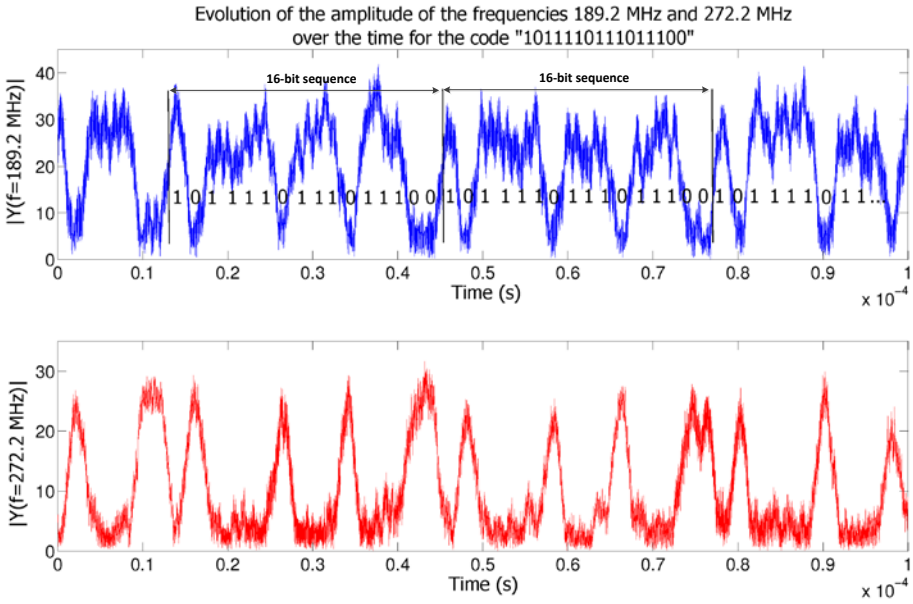

Fig. 4. Coherent demodulation of the 16-bit code word cyclically sent by the BFSK transmitter at 500 Kbps, the top (bottom) graph corresponds to the spectral contribution of signal at f_1 (f_0).

V. Comparison with state of the art spy circuitries using a side-channel

Table II compares the implementation of the proposed ultra-lightweight BFSK transmitter with other recently published state of the art methods. Table II gives the spy circuitry application (*App.*) for each reference; this may be IP protection (*IPP*) or hardware Trojan (*HT*) or both (for the presented work, *PW*). In addition, Table II gives the year of publication (*YoP*), the side channel used, the hardware resources required only for the leakage generator (for example we do not take the hardware used for IP watermark generation or the Trojan's payload into account). Unfortunately, the principles compared do not use the same hardware. For the sake of correctness, we give the implementation results as they are presented in the referenced papers. Nevertheless, the implementation bitrate of these previously published works can be roughly compared with our proposed solution. Based on published data, we computed the bitrate of all the proposals by using the number of clock cycles needed to send information via the side channel. For all the references presented in this table, the bitrate was computed using a 500 KHz frequency for data synchronization (same frequency is used for data transmission in Fig. 4).

TABLE II
SUMMARY OF CHARACTERISTICS OF SPY CIRCUITRIES EXPLOITING SIDE-CHANNELS

App.	Ref.	YoP	Side channel	Hardware resources	Target	Bit rate (@500 KHz)
IPP	[5]	2008	Thermal emanation	255 Spartan-3 slices	Xilinx Spartan-3	7.10^{-3} bps
	[6]	2008	Power consumption	16 * 16-bit circular shift-registers	Xilinx Spartan-3 and Virtex-II	200 bps
	[7]	2010	Power consumption	16-bit circular shift-register	Xilinx Virtex-II Pro	500 bps
HT	[9]	2009	Power consumption	8 parallel D-flip-flops or 16-bit circular shit register	Xilinx Spartan-3E and Virtex-II Pro	485 bps
	[10]	2013	Power consumption	16-bit circular shift-registers per bit	Xilinx Virtex-5	976 bps
Both	PW	2015	Electro-magnetic emanation	1 configurable ring-oscillator (like a D-flip-flop in ASIC)	Microsemi Fusion	500 Kbps

As can be seen in Table II, the proposed work reaches the highest bitrate. The reason for such a good performance is first that we use a spectral analysis of the local electromagnetic leak based on a simple frequency modulation. Except for [4], all the other solutions use a global measurement of power consumption, which reduces the signal-to-noise ratio of the information leaked via the side channel. Our proposal is clearly the smallest spy circuitry ever published. Although solutions based on circular shift-registers are well adapted to last generation FPGA families, since the 16-bit shift registers can be designed using only one look-up table, they are not suitable for ASIC technologies. Currently, an ASIC implementation of a 16-bit shift register requires 16 flip-flops whereas the solution we propose occupies an area equivalent to only one D-flip-flop.

In this paper, we present the proposed spy circuitry for IP protection, but it can also be used for hardware Trojan. Most of the other proposals could also be used for both applications. Note that in 2012, Kasper et al. proposed to use the work initiated in [9] for hardware Trojan or IP watermarking implementation [19]. However, by using electromagnetic emanation and a configurable ring oscillator, the proposed solution is the most convincing for industrial applications (e.g., those aimed at IP protection) because of its very small area and high bitrate.

VI. Industrial scenarios using the proposed IP protection

According to the previous section, in comparison with other works, our propose goes clearly towards using a spy circuit in an industrial context for IP protection. Two industrial scenarios are presented in the following.

The first scenario is the identification of embedded IP in the supply chain. This identification is used in order to be sure to don't use counterfeiting (fake) devices. In recent years, the issue of counterfeiting of integrated circuits has increased considerably. For example, the number of counterfeit electronic circuits collected by U.S. Customs from 2001 to 2011 has increased by around 700 [20]. Between 2007 and 2010, U.S. Customs collected 5.6 million counterfeit electronic products [21]. Overall, the estimation of counterfeiting is about 7% of the semiconductor market [22] which represented a loss of about $ 22 billion in 2014 for the legal industry.

It is therefore crucial and strategic to be able to detect counterfeit IC as soon as possible in the supply chain (this is particularly crucial for military and space grad devices). Fig. 5 shows a possible framework to manage the device under test (control the enable signal) and check the IP identification by using an EM probe, an amplifier and a dedicated acquisition system including a spectral analysis and the proposed demodulation method. Due to the high bit rate of the proposition solution the identification of the ID requires less than 1ms (with 500Kps bit rate as in Fig 4.). This counterfeiting detection could be completed by other physical (invasive or not) and optical inspection [23].

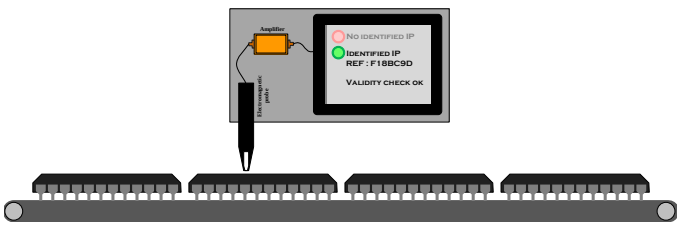

Fig. 4. Rapid and contactless IP identification in the supply chain by using EM transmission of IP ID.

The second scenario occurs when a IP designers would like to verify the illegal presence of its IP inside a device (ASIC or FPGA). In this case the proposed transmitter provides to the

identification scheme a data like a PUF [24] or a watermarking. Watermarking is a technique of steganography which provides the ownership of an IC (or an IP) by checking for the presence of hidden information called the watermark [3]. Most of the watermarking methods proposed in the literature need a complex verification scheme. Nevertheless it is possible to use power consumption as proposed in [8] and [3] but it is easy and cheap to use global countermeasure in order to mask the power consumption due to the watermark [25]. Using electromagnetic emanation in this scenario is better because as electromagnetic emanation is local it is really hard to mask it by using a global countermeasure. Moreover, in this paper we have shown that due to the SNR of BFSK signal, it is unrealistic to try to detect it without the precise knowledge of the used frequencies for data transmission.

VII. Conclusion

IP protection has become crucial topics for hardware security due to the lack of trust in IP market. In this paper, we have presented an ultra-lightweight transmitter of IP identity using the electromagnetic side channel. Based on a configurable ring oscillator, our solution exploits a BFSK signal to transmit information by way of the electromagnetic channel. By performing a slippery window spectral analysis of the near field electromagnetic emanations captured locally over the BFSK transmitter circuitry, the proposed transmission achieves a high bitrate (experimentally 500 Kbps and theoretically limited to 53 Mbps with a Microsemi Fusion FPGA), which has not been achieved before. Moreover, the transmitter occupies very small area. For the highest frequency and data rate, our solution requires 4.67 equivalent gates, which it is less than the requirement of a small D-flip-flop. Such a small requirement of logical resources makes reverse engineering of the chip very difficult and detection of the transmitter using standard Trojan detection methods is not feasible.

Acknowledgment

The work presented in this paper was realized in the frame of the SALWARE project number ANR-13-JS03-0003 supported by the French ”Agence Nationale de la Recherche”and by the French “Fondation de Recherche pour l’Aéronautique et l’Espace”.

References

[1] B. Colombier, L. Bossuet, "Survey of hardware protection of design data for integrated circuits and intellectual properties," Computers & Digital Techniques, IET, vol.8, no.6, pp.274,287, 2014.

[2] C. Marchand, L. Bossuet, E. Jung, "IP watermark verification based on power consumption analysis," In Proceedings of the 27th IEEE International System-on-Chip Conference, SOCC 2014, pp. 330-335, 2014.

[3] P. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis”, in Wiener M. (Ed.), Proceedings of the 19th Annual International Cryptology Conference, CRYPTO 1999, Springer, Lecture Note on Computer Science, vol. 1666, pp. 388-397, 1999.

[4] N. Kamoun, L. Bossuet, A. Gazel, “Experimental Implementation of 2ODPA attacks on AES design with flash-based FPGA Technology,” in proceedings of the 22nd IEEE International Conference on Microelectronics, IMC 2010, pp. 407-410, 2010.

[5] C. Marsh, T. Kean, D. Mclaren, “Protecting designs with a passive thermal tag,” In Proceedings of the 15th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2008, pp.218-221, 2008.

[6] D. Ziener, J. Teich, “Power Signature Watermarking of IP Cores for FPGAs,” Journal of Signal Processing Systems, Springer, vol. 51, pp. 123-136, 2008.

[7] G. T. Becker, M. Kasper, A. Moradi and C. Paar, “Side-channel based watermarks for integrated circuits,” In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2010, pp. 30-35, 2010.

[8] S. Kerckhof, F. Durvaux, F.X. Standaert, and B. Gérard, “Intellectual Property Protection for FPGA Designs with Soft Physical Hash Functions: First Experimental Results,” In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013, pp. 7-12, 2013.

[9] L. Lin, M. Kasper, T. Güneysu, C. Paar, W. Burleson, “Trojan Side-Channels: Lightweight hardware Trojans through Side-Channel Engineering”, In Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, CHES 2009, Springer, Lecture Notes in Computer Science, vol. 5747, pp. 382-395, 2009.

[10] S. Kutzner, A. Poschmann, and M. Stöttinger, “TROJANUS: An Ultra-Lightweight Side-Channel Leakage Generator for FPGAs”, In Proceedings of International Conference on Field-Programmable Technology, ICFPT 2013, pp. 160-167, 2013.

[11] J.F. Gallais, J. Großschädl, N. Hanley, M. Kasper, M. Medwed, F. Regazzoni, J.M. Schmidt, S. Tillich, and M. Wójcik, “Hardware Trojans for Inducing or Amplifying Side-Channel Leakage of Cryptographic Software,” In Proceedings of the Second International Conference on Trusted Systems, INTRUST 2010, pp. 253-270, 2010.

[12] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, “EM leakage analysis on True Random Number Generator: Frequency and localization retrieval method”, in Proceedings of the Asia Pacific International Symposium and Exhibition on Electromagnetic Compatibility, APEMC 2013, 2013.

[13] Virtual Silicon Inc. 0.18 µm VIP Standard Cell Library Tape Out Ready, Part Number: UMCL18G212T3, Process: UMC Logic 0.18 µm Generic II Technology: 0.18µm, 2004.

[14] P. Kitos, Y. Zhang (Eds.), “RFID Security – Techniques, Protocols and System-on-Chip (1st ed.)” Spinger Publishing compagny, 2008.

[15] R. Torrance, and D. James, “The state-of-the-art in semiconductor reverse engineering,” In Proceedings of the 48th Design Automation Conference, DAC 2011, ACM/EDAC/IEEE , pp. 333-338, 2011

[16] P. Subramanyan, N. Tsiskaridze, W. Li, A. Gascon, W. Tan, A. Tiwari, N. Shankar, S. Seshia, and S. Malik, “Reverse Engineering Digital Circuits Using Structural and Functional Analyses,” in IEEE Transactions on Emerging Topics in Computing, 2013.

[17] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B Sunar, “Trojan Detection using IC Fingerprinting” in Proceedings of the IEEE Symposium on Security and Privacy, pp. 296-310, 2007.

[18] Y. Jin, and Y. Makris, “Hardware Trojan Detection using Path Delay Fingerprint” in IEEE International Workshop on Hardware-Oriented Security and Trust, HOST 2008, pp. 51-57, 2008.

[19] M. Kasper, A. Moradi, G.T. Becker, O. Mischke, T. Güneysu, C. Paar and W. Burleson, “Side Channels as Building Blocks”, In Journal of Cryptography Engineering, Springer, vol. 2, no. 3, pp. 143-159, 2012.

[20] C. Gorman, “Counterfeit Chips on the Rise,” IEEE Spectrum, June 2012.

[21] AGMA, Alliance for Gray Markets and Counterfeit Adatement, http://www.agmaglobal.org

[22] M. Pecht, and S. Tiku, “Bogus! Electronic manufacturing and consumers confront a rising tide of counterfeit electronics,” IEEE Spectrum, May 2006.

[23] M. Tehranipoor, U. Guin, D. Forte. Counterfeit Integrated Circuits - Detection and Avoidance. Springer, 2015.

[24] L. Bossuet, X. T. Ngo, Z. Cherif, V. Fischer. A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon. IEEE Transactions on Emerging Topics in Computing, Vol. 2, Issue 1, pp. 30-36, 2014.

[25] N. Kamoun, L. Bossuet, and A. Ghazel, “Correlated Power Noise Generator as a Low Cost DPA Countermeasure to Secure Hardware AES Cipher,” In Proceedings of the International Conference on Signals, Circuits and Systems, SCS 2009, pp. 1-6, 2009.